Published and Copyright (c) 1999 - 2016
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1808 02/26/16

~ Teenage Hacker Arrested ~ People Are Talking! ~ 'Necropolis' Is Coming!

~ CMU Hacked Tor Users! ~ Linux Mint Site Hacked ~ Howard Scott Warshaw!

~ NSA Data Center Attacks ~ Facebook "Reactions"! ~ Dave Needle Passes Away

~ Google’s Project Shield ~ Siri for Mac Is Coming ~ MouseJack Hack Risk!

-* Nathan Drake’s Last Hurrah! *-
-* Zuckerberg, Dorsey Are Threatened! *-
-* Brit Intelligence Allowed To Hack Anyone! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

In case you haven’t been receiving your weekly issue of A-ONE via our subscriber list, we apologize. I’ve learned that there have been some server changes and moves, and now there are some problems with the server itself. These issues are being dealt with, and hopefully will be resolved quickly (if not already!). Meanwhile, there are other routes to find the magazine. I know, if you don’t see these comments, how are you to know??!!

Anyway, the political world - at least our par of it - is taking on new meanings. I found a quote today from Sen. Lindsey Graham to be quite comical. According to the article: Sen. Lindsey Graham is so disgusted with the GOP’s embrace of Donald Trump, he says: "My party has gone batshit crazy."

Apparently, Senator, many Americans are tired of "politics as usual" and they are making their voices (and votes) heard. Frankly, I’m surprised at how well Donald Trump is doing. Or, is it more correct to say how poorly the other GOP candidates are doing? And on the Democrats side, look how well Bernie Sanders is doing? Looks like mainstream politics is facing a voter revolution of sorts.

Here we are, the last week of February, and no snow on the ground! After last winter, you won’t hear any complaints from me about the lack of snow! The weather has been crazy on the East Coast lately, with all kinds of nasty weather in the South and mid-Atlantic, but we’ve been pretty fortunate here in the Northeast. I hope that March continues with this trend!

Until next time...

=~=~=~=

->In This Week’s Gaming Section - ’Uncharted 4’ Creators Plot Nathan Drake’s La st Hurrah!
""""""""""""""""""""""""""""""" Bandai Namco Brings ’Necropolis’ to PS4, Xbox One!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""

’Uncharted 4’ Creators Plot Nathan Drake’s Last Hurrah

The creators of "Uncharted 4" much like cliff-diving, treasure-hunting series protagonist Nathan Drake aren’t afraid to take a few risks.

With the release of "Uncharted 4: A Thief’s End" on April 26, directors Neil Druckmann and Bruce Straley are ending the smart-alecky fortune hunter’s story at the peak of the franchise’s popularity. Since the release of the original "Uncharted: Drake’s Fortune" in 2007, publisher Sony has sold more than 21 million copies of the "Uncharted" series.

"It’s time," said Druckmann during a recent visit to developer Naughty Dog’s offices. "Sometimes, a character just lets you know it’s time to move on. For me, that was part of the intrigue of coming back to this world. You never see something successful in the industry end. It usually just fizzles out."

After working on the first pair of "Uncharted" games and the apocalyptic saga "The Last of Us," Druckmann and Straley were brought onto "Uncharted 4" after "Uncharted 3" directors Amy Hennig and Justin Richmond departed the studio. Druckmann said the game’s story changed "100 percent" when they took over the project, the first new "Uncharted" installment for the PlayStation 4.

"This is the biggest, most ambitious ’Uncharted’ let alone game that Naughty Dog has ever endeavored to take on," said Straley. "We want to do this justice. We want it to be a mind-blowing, eye-popping, sweaty-palms adventure. Everybody is bleeding out of their eye sockets to make it come together. We want to make sure Drake is sent off properly."

"Uncharted 4" finds Drake (played by Nolan North) retired from his continent-hopping career until his thought-to-be-dead brother Sam (Troy Baker) shows up seeking his help. Their reunion puts Drake’s relationship with journalist Elena Fisher (Emily Rose) in jeopardy. ("If you’re done lying to me, then you should stop lying to yourself," she cautions him in the game’s most recent trailer.) For the developers, the introduction of Drake’s long-lost brother provided them with a unique storytelling opportunity.

"It’s a way for us to get into Drake’s past," said Druckmann. "This is someone who knows things about Nathan Drake that no one

else knows. We’re flashing back to when the two brothers were young. They haven’t seen each other for 15 years. It’s a way for us to lure Nate back into the world of adventure. As they go further, we’ll explore their differences."

The daring decree to conclude Drake’s tale isn’t the only bold choice made by the Naughty Dog team. The creators also controversially cast a white actress to portray a black villain in "Uncharted 4."

On-screen, Drake’s adversary Nadine Ross looks like a black South African private military contractor. However, she’s portrayed in the real world with a vocal- and motion-capture performance by Caucasian actress Laura Bailey, who worked with a dialect coach on a South African accent and was cast before developers finalized the character’s look.

"The easy thing to do at that point to avoid any controversy would’ve been to say, ’Let’s make her white,’" said Druckmann. "No one would’ve questioned it or knew there was another option. Instead, we moved forward with the concept for this really strong character of color that you don’t see often in a game with this person we already cast who was great in this role."

Druckmann said "it just felt right" when Bailey’s performance and the designers’ visuals were merged together on-screen. Conversely, Druckmann said they also cast a black actor to portray a white character before his appearance was locked down, although he declined to specify the actor or role.

"It probably won’t be revealed until the game is out," he said.

The release of "Uncharted 4" will mark the end of a rollicking journey that began over eight years ago when Druckmann and Straley worked on the first "Uncharted" entry. As soon as "Uncharted 4" is shipped, Druckmann has his own adventure planned.

"I promised my daughter I would take her to Disneyland," he said. "That’s what I’m going to do."

’Dark Souls’ Publisher Brings ’Necropolis’ to PS4, Xbox One

Here’s one to add to your video game watch list: Necropolis is a stylish, hardcore dungeon-diving game from Harebrained Schemes, the studio behind the magnificent cyberpunk title Shadowrun Returns. It was originally due to hit PC and Mac on March 17th, but now Dark Souls publisher Bandai Namco is involved and the times, they are a-changing.

Necropolis is now due to hit PC, Mac, PlayStation 4 and Xbox One in the summer, with Bandai handling the console publishing duties. Harebrained Schemes is self-publishing the game on Steam.

"While we really hate to slip a release date, we know from experience that doing a console release right adds a significant amount of development work," Harebrained Schemes President Mitch

Gitelman says in a press release. "So we believe this is absolutely the right decision, and that the additional time will make for an even better Necropolis for consoles and for PC."

Necropolis is an action title where players have just one life to defeat hordes of ghastly beasties in ever-changing, procedurally generated dungeons. It features crafting and four-player drop-in co-op, plus an art style that is both moody and adorable at the same time. It looks like an effortlessly cool game, which should make it perfect for the summer.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!

Amiga Engineer, Atari Lynx Co-creator, Dave Needle, Passes Away

Dave Needle, an instrumental figure in the completion of the Lorraine project, which resulted in the Amiga 1000, passed away on Saturday, February 20.

Needle was one of the main engineers behind the Amiga’s custom chips, and later on went on to co-create the Atari Lynx - the first handheld system to feature a color LCD screen - in the late 80s.

Needle was also the co-inventor of the 3DO Interactive Multiplayer home console, a short-lived, but cutting edge system created by himself, designer R.J. Mical, and EA founder Trip Hawkins.

News of Needle’s death was posted on Facebook by the Atari History Book team over the weekend, although no cause was given.

The Man Who Made ’The Worst Video Game in History’

The video game of Steven Spielberg’s ET is considered to be one of the worst of all time and has even been blamed for triggering the collapse of Atari. Howard Scott Warshaw, the gifted programmer who made it, explains how it was rushed out in a matter of weeks - and how he feels about those events in California now.

Spielberg was unimpressed.

"Couldn’t you do something more like Pac-Man?" he asked.

It was July 1982 and Atari, then one of the world’s most successful tech companies, had just paid a reported $21m for the video game rights to Spielberg’s new blockbuster, ET the Extra-Terrestrial.

Howard Scott Warshaw was the programmer tasked with designing the game.

"I was stunned," says Warshaw. "Here was Steven Spielberg, one of my idols, suggesting that I knock off the game! My impulse was to go, ’Well, gee, Steven, couldn’t you make something more like The Day The Earth Stood Still?’"

Warshaw’s stock was high at Atari. The 24-year-old had just finished the video game of Spielberg’s Raiders of the Lost Ark. Spielberg considered Warshaw a "certifiable genius" and 36 hours earlier Warshaw had been hand-picked for their next collaboration.

"It was a day that will live in infamy in my life forever," says Warshaw. "I was sitting in my office and I get a call from the Atari CEO. He said, ’Howard, we need the ET video game done. Can you do it?’

"And I said, ’Absolutely, yes I can!’"

Games for the Atari 2600 were distributed on cartridges that took weeks to manufacture. If ET was to be in the shops for Christmas, Warshaw had a tight deadline.

"The CEO goes, ’We need it for 1 September.’ That left five weeks to do it! Normally it’d be six to eight months to do a game, not five weeks.

"Then he said, ’Design the game and on Thursday morning, be at the airport and there will be a Learjet waiting to take you to see Spielberg.’

"I’m not sure exactly what I was full of but whatever it was, I was overflowing with it."

Warshaw drew up his pitch to Spielberg, and travelled from the Atari headquarters in Sunnyvale, California to Los Angeles. His idea was an adventure game in which the player had to help ET phone home by collecting components to make an inter-planetary telephone. The player would have to dodge government agents and scientists in order to complete the mission.

"I got down to Spielberg and I laid out the whole design," he says. "I told him, ’I think it’s really important that we do something innovative. ET is a breakthrough movie and I think we need a breakthrough game.’

"I talked him out of the idea of a Pac-Man knock-off. But the key was to design a game that I could deliver in five weeks."

Atari needed ET to be a hit. In 1982 sales had reached a peak of $2 billion but the company was losing market share to home computers like the Commodore 64, which could do more than play games.

"It was the hardest I’ve ever worked on anything in my life," says Warshaw, who was the game’s sole programmer. "I started working at the office but after a while I realised there was a

problem; I still have to go home to sleep and eat occasionally.

"So we had another development system installed in my house so that I would never be more than two minutes away from working on the code except when I was driving.

"There was a manager who was assigned to make sure I was eating so that I'd be able to keep going.

"When it came to the end of the process, my reaction was, 'Wow, I did it!'"

Atari ordered an initial run of four million copies and budgeted a reported $5m on what would be, at the time, the biggest-ever advertising campaign for a video game.

"ET needs help from his human friend - and that's you!" read the magazine ad. Television commercials ran for weeks. Spielberg himself appeared in a promotional video, whilst Warshaw was flown to the London premiere of ET and given a seat in front of the Princess of Wales.

"The bosses believed that as long as we put anything out the door with ET's name on it would sell millions and millions," he says.

To begin with, the game was "right up there on the Billboard top sellers" but word began to spread that there were serious problems.

"It was a finished game but it certainly wasn't perfect," Warshaw says. "There were too many opportunities where you could suddenly wind up in an odd situation. That was too much for a lot of people and caused them to put the game down."

Players complained that the ET character would inexplicably fall into pits and get stuck. As one 10-year-old told The New York Times: "It wasn't fun."

Atari soon realised that ET was not going home. In early December 1982 it announced "disappointing" sales for the year and the value of its parent company Warner Communications plunged. The results triggered steep drops in the value of other video game makers.

"After the Christmas season it was starting to come back from retailers," says Warshaw. "It still sold nearly 1.5 million units, but when you needed to sell four million, that's not good enough."

By the second quarter of 1983, Atari's parent company announced losses of $310m.

"Things just started to unravel," says Warshaw. "It's awesome to be credited with single-handedly bringing down a billion-dollar industry with eight kilobytes of code. But the truth is a little more complex."

Consumers were turning to the home computer and the market was saturated with video games. In a bid to avoid collapse, prices - and much of the workforce - were slashed. But it was futile and in July 1984 Warner offloaded Atari for $240m.

"I took some time off to recover from the whole experience," says Warshaw. "I went into real estate for a couple of years and hated it.

"Eventually I went back to technology, returning to video games as a manager and director, but it had lost the charm by then."

Creatively unfulfilled, Warshaw undertook projects in writing and TV production.

"I knew I was done with the industry but I couldn’t envision an alternative. I became depressed."

Warshaw’s solution was "to throw reason to the wind" and in 2008 he retrained as a psychotherapist.

"Maybe a part of me really wanted to compensate for all the trauma and depression I created with the ET game," he says. "But in reality it’s something I always wanted to do."

Today Warshaw bills himself as The Silicon Valley Therapist, "fluent in both English and nerd". Does he use his own story of colossal failure with clients?

"Sometimes I do," he admits.

"But every therapist uses their own experience with their clients. To me it’s a very natural thing. Programmers and therapists are all systems analysts. It’s just that I’ve moved on to a much more sophisticated hardware."

In April 2014 Warshaw was given his own chance to obtain closure on the ET fiasco. A film company was making a documentary about a legend that had persisted for 30 years - that in 1983 Atari had buried truckloads of the unsold ET games in the New Mexico desert.

"I never believed it, I just thought it was absurd," says Warshaw.

The city of Alamogordo granted permission for a public excavation to take place. Warshaw was invited to attend.

"When we arrived, there was a long, long line of fans from all over the country who had travelled to see this," he says. "It was an odd thing to sit there and literally watch your past being dug up."

The excavation confirmed that Atari products were indeed buried at the dump and Warshaw was filmed at the moment a battered and crushed copy of ET was pulled from the ground.

"I became extremely emotional," he says. "This little game that I had written in five weeks more than 30 years ago was still generating excitement. I was full of gratitude.

"Is ET really the worst game of all time? Probably not. But the story of the fall of the video game industry needed a face and that was ET.

"I actually prefer it when people do identify it as the worst game of all time because I also did Yars Revenge and that’s

frequently identified as one of the best of all time. So between the two, I have the greatest range of any designer in history!"

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

British Intelligence Is Legally Allowed to Hack Anyone

Hacking of computers, smartphones and networks in the United Kingdom or abroad by the Government Communications Headquarters (GCHQ) is LEGAL, the UK's Investigatory Powers Tribunal (IPT) ruled.

So, the UK is giving clean chit to its intelligence agency to spy on its people as well as people living abroad.

Now, how is that okay?

The British spying nerve center GCHQ has won a major court case in defense of the agency's persistent hacking programs.

After revelations by NSA whistleblower Edward Snowden about the extent of spying by the US and the UK, Privacy International and seven Internet Service Providers (ISPs) launched a legal challenge against the GCHQ's hacking operations.

The case alleged that the British spying agency was breaking European law and violating fundamental warrant protections by its too intrusive and persistent surveillance actions.

Though GCHQ "neither confirm nor deny" the existence of such operations, the case made headlines in December last year when GCHQ admitted to its persistent hacking programs, "within and outside the UK," for the first time during the case hearings.

However, a panel of five members of the IPT handed down the judgment on Friday, ruling that the computer network exploitation that may involve activating microphones and cameras on devices remotely without the owner's knowledge is legal and does not breach human rights.

According to the senior judges, GCHQ's hacking efforts had "raised a number of serious questions," but a "proper balance" has been struck between the privacy of individuals and the need of the intelligence agency to investigate crimes.

Here's what the lengthy ruling [PDF] from the Investigatory Powers Tribunal (IPT) reads:

"The use of computer network exploitation by GCHQ, now avowed,

has obviously raised a number of serious questions, which we have done our best to resolve in this Judgment.

Plainly it again emphasises the requirement for a balance to be drawn between the urgent need of the Intelligence Agencies to safeguard the public and the protection of an individual's privacy and/or freedom of expression."

The agency's hacking efforts had allowed the agents to tap into almost any electronic equipment, including computers, servers, routers, laptops, mobile phones and even Internet of Thing (IoT) devices such as smart toys, smart TVs and more.

GCHQ also said it had:

Installed malware
Remotely turned ON cameras and microphone
Installed Keylogger that records every pressed key on a keyboard
Tracked suspects' locations via GPS
Remotely stole documents from target devices

Privacy International, which brought the case, is, of course, very disappointed with the ruling, and so are we. How could a country decide spying people outside its country?

The group will be challenging the decision on the grounds that it fragmented the European Convention on Human Rights when it comes to spying people within but outside of the UK.

"This case exposed not only these secret practices but also the undemocratic manner in which the Government sought to backdate powers to do this under the radar," Scarlet Kim, legal officer at London-based Privacy International said in a statement.

"Just because the Government magically produces guidelines for hacking should not legitimize this practice."

However, British Foreign Secretary Philip Hammond, welcomed the ruling, saying the ruling was fair and took into account invasive actions that are necessary for the security of UK.

"Once again, the law and practice around our Security and Intelligence Agencies capabilities and procedures have been scrutinized by an independent body and been confirmed to be lawful and proportionate," Hammond said.

So, once again the threat of terrorism saved the GCHQ's ass, as the judgement says the capabilities operated by the agency lie "at the very heart of the attempts of the State to safeguard the citizen against terrorist attack."

Hackers Associated with ISIS Threaten Mark Zuckerberg, Jack Dorsey

The video comes as the two companies step up anti-terrorism efforts.

A video made by a group of ISIS supporters threatens Facebook CEO Mark Zuckerberg and Twitter CEO Jack Dorsey.

The 25-minute video, made by an ISIS-affiliated hacker group calling itself the Sons of the Caliphate Army, came in response to recent efforts by the two tech companies to rid their platforms of terrorists, according to The Wall Street Journal.

The video shows Zuckerberg and Dorsey s pictures engulfed in flames and covered in bullet holes, though it never explicitly threatens their lives. It also shows screenshots of ISIS fighters accounts on the platforms, as if to boast that the companies attempts to shut down terrorist profiles aren t making headway.

At the end of the video, the Journal reports that the group writes this: To Mark and Jack, founders of Twitter and Facebook and to their Crusader government. You announce daily that you suspended many of your accounts, and to you we say: Is that all you can do? You are not in our league.

Earlier this month, Twitter announced it had deleted 125,000 accounts associated with the terrorist group in the previous six months. And on Wednesday, Apple, Twitter, Snapchat, Facebook, and other tech teams gathered at the Department of Justice to discuss strategies to combat ISIS rhetoric and recruiting online.

Dorsey was also threatened by the group in a video last year.

Judge Confirms Government Paid CMU Scientists To Hack Tor Users for FBI

Everything is now crystal clear:

The security researchers from Carnegie Mellon University (CMU) were hired by the federal officials to discover a technique that could help the FBI Unmask Tor users and Reveal their IP addresses as part of a criminal investigation.

Yes, a federal judge in Washington has recently confirmed that the computer scientists at CMU’s Software Engineering Institute (SEI) were indeed behind a hack of the TOR project in 2014, according to court documents [PDF] filed Tuesday.

In November 2015, The Hacker News reported that Tor Project Director Roger Dingledine accused the Federal Bureau of Investigation (FBI) of paying the CMU, at least, $1 Million for providing information that led to the criminal suspects identification on the Dark Web.

After this news had broken, the FBI denied the claims, saying "The allegation that we paid [CMU] $1 Million to hack into TOR is inaccurate."

Meanwhile, the CMU also published a press release, saying the university had been subpoenaed for the IP addresses it obtained during its research.

The revelation came out as part of the ongoing case against Brian

Richard Farrell, an alleged Silk Road 2 lieutenant who was arrested in January 2014. It has emerged that the federal officials recruited a "university-based research institute" that was running systems on the Tor network to help authorities uncover the identity of Farrell.

Now, a recent filing in one of the affected criminal cases has confirmed both the name of the "university-based research institute" and the existence of a subpoena.

Some earlier allegations by the TOR project seem to be wrong. The research was funded by the Department of Defense, which was later subpoenaed by the FBI.

Here’s what the Tuesday court order, by US District Judge Richard Jones, filed in the case of Farrell reads:

"The record demonstrates that the defendant’s IP address was identified by the Software Engineering Institute (SEI) of Carnegie Mellon University (CMU) when SEI was conducting research on the Tor network which was funded by the Department of Defense (DOD)."

"Farrell’s IP address was observed when SEI was operating its computers on the Tor network. This information was obtained by law enforcement pursuant to a subpoena served on SEI-CMU."

Farrell is charged with conspiracy to distribute drugs like cocaine, heroin, and methamphetamine through the Silk Road 2.0 dark web marketplace.

Last summer, the DoD renewed a contract worth over $1.73 Billion with the SEI, which according to CMU, is the only federally funded research center that focus on "software-related security and engineering issues."

Carnegie Mellon University’s SEI came under suspicion for the TOR hack due to the sudden cancellation of the talk from SEI researchers Michael McCord and Alexander Volynkin on de-anonymizing Tor users at Black Hat 2014 hacking conference.

More details on the matter are still unclear, but the judge confirmed few facts about the TOR and stated that "Tor users clearly lack a reasonable expectation of privacy in their IP addresses while using the Tor network."

NSA Data Center Experiencing 300 Million Hacking Attempts Per Day

Utah State computer systems are experiencing a massive cyber attack on up to 300 Million Hacking attempts per day due to National Security Agency s (NSA) data center in the state.

Yes, 300,000,000 hacking attempts in a day!

According to the statistical survey, it is evident that the computer systems in the US State of Utah began to experience the hacking attack a few years back, precisely, soon after the NSA revelations by global surveillance whistleblower Edward Snowden.

It is a less-known fact that the NSA has built its new data center near the city of Bluffdale, Utah. However, a couple of years back, when Snowden revealed the presence of the data center, the attacks have constantly been going on.

The PRISM spying program by Big Brothers at NSA might have shifted the attention of hackers for the retaliation against mass-surveillance and flared up this heightened cyber attacks against the spying agency.

According to Utah Commissioner of public safety, Keith Squires, as quoted by KUTV:

"In 2010, my IT director was letting me know that the number of attacks we were averaging a day was between 25,000 to 80,000. We had peaks in the past year or so that were over 300,000,000 a day."

Additionally, advanced weapons systems at Hill Air Force Base and other tech companies in Utah could also be the reason for this fueling cyber attacks.

The Security officers had identified the sudden influx of IP traffic traced into foreign IP ranges and said the incident would be a model of a botnet attack.

The botnet network scans for the technical glitches in the communication pathways to infect the system, as per its Command and Control (C&C) instructions.

In an attempt to minimize the attacking vector, Utah Security Officer had blocked the IP addresses from China, Russia, and Indonesia.

In the majority of cases, hackers are trying to gain a single access by many tactical ploys that could lead them to land into the NSA mainframes.

The Big Brother is Watching you !

Warning Linux Mint Website Hacked and ISOs Replaced With Backdoored Operating System

Are you also the one who downloaded Linux Mint on February 20th? You may have been Infected!

Linux Mint is one of the best and popular Linux distros available today, but if you have downloaded and installed the operating system recently you might have done so using a malicious ISO image.

Here’s why:

Last night, Some unknown hacker or group of hackers had managed to hack into the Linux Mint website and replaced the download links on the site that pointed to one of their servers offering a malicious ISO images for the Linux Mint 17.3 Cinnamon Edition.

"Hackers made a modified Linux Mint ISO, with a backdoor in it, and managed to hack our website to point to it," the head of Linux Mint project Clement Lefebvre said in a surprising announcement dated February 21, 2016.

Who are affected?

As far as the Linux Mint team knows, the issue only affects the one edition, and that is Linux Mint 17.3 Cinnamon edition.

The situation happened last night, so the issue only impacts people who downloaded the above-mentioned version of Linux Mint on February 20th.

However, if you have downloaded the Cinnamon edition or release before Saturday 20th, February, the issue does not affect you. Even if you downloaded a different edition including Mint 17.3 Cinnamon via Torrent or direct HTTP link, this does not affect you either.

What had Happened?

Hackers believed to have accessed the underlying server via the team’s WordPress blog and then got shell access to www-data.

From there, the hackers manipulated the Linux Mint download page and pointed it to a malicious FTP (File Transfer Protocol) server hosted in Bulgaria (IP: 5.104.175.212), the investigative team discovered.

The infected Linux ISO images installed the complete OS with the Internet Relay Chat (IRC) backdoor Tsunami, giving the attackers access to the system via IRC servers.

Tsunami is a well-known Linux ELF trojan that is a simple IRC bot used for launching Distributed Denial of Service (DDoS) attacks.

However, the Linux Mint team managed to discover the hack, cleaned up the links from their website quickly, announced the data breach on their official blog, and then it appears that the hackers compromised its download page again.

Knowing that it has failed to eliminate the exact point of entry of hackers, the Linux Mint team took the entire linuxmint.com domain offline to prevent the ISO images from spreading to its users.

The Linux Mint official website is currently offline until the team investigates the issue entirely. However, the hackers’ motive behind the hack is not clear yet.

"What we don’t know is the motivation behind this attack. If more efforts are made to attack our project and if the goal is to hurt us, we ll get in touch with authorities and security firms to confront the people behind this," Lefebvre added.

The hackers are selling the Linux Mint full website’s database for a just $85, which shows a sign of their lack of knowledge.

The hack seems to be a work of some script kiddies or an inexperienced group as they opted to infect a top-shelf Linux distro with a silly IRC bot that is considered to be outdated in early 2010. Instead, they would have used more dangerous malware like Banking Trojans.

Also, even after the hack was initially discovered, the hackers re-compromised the site, which again shows the hackers' lack of experience.

Here's How to Protect your Linux Machine

Users with the ISO image can check its signature in an effort to make sure it is valid.

To check for an infected download, you can compare the MD5 signature with the official versions, included in Lefebvre's blog post.

If found infected, users are advised to follow these steps:

- Take the computer offline.
- Backup all your personal data.
- Reinstall the operating system (with a clean ISO) or format the partition.
- Change passwords for sensitive websites and emails.

Hackers Can Break Into Your Computer Through Your Wireless Mouse

It turns out that even something as seemingly benign as your mouse can put your personal information at risk. That s according to a report by security firm Bastille, which says that hackers could in theory take control of your computer through its wireless peripherals.

The hack, which the company calls MouseJack, affects nearly every wireless mouse and keyboard on the market and could give a hacker complete access to your personal computer or to the network at your office.

The hack isn t exactly sophisticated either. According to Bastille, all a would-be hacker needs is about $15 worth of computer hardware, which he could then use to send commands from his computer to yours.

The hack works because while your wireless keyboard sends information in encrypted form to your computer s wireless dongle (so hackers can t see what you re typing), your mouse doesn t.

As a result, hackers can send signals designed to perform keyboard commands to your dongle. Those signals can then be used to hijack your system.

Wireless mice and keyboards are the most common accessories for PCs today, and we have found a way to take over billions of them, said Marc Newlin, Bastille s engineer responsible for the MouseJack discovery, in a statement.

So how to protect yourself? Well, some wireless mouse and keyboard manufacturers developed their devices so they can be patched via firmware updates. Other companies offerings, however, can t be updated and will simply have to be replaced.

Fortunately, Bastille has published a list of the impacted hardware, as well as information about how some peripherals companies have responded to the hack.

Police Arrest 16-year-old Boy Who Hacked CIA Director

The teenage hacker, who calls himself a member of hacktivist group "Cracka with Attitude," behind the series of hacks on the United States government and its high-level officials, including CIA director, might have finally got arrested.

In a joint effort, the Federal Bureau of Investigation (FBI) and British police reportedly have arrested a 16-year-old British teenager who they believe had allegedly:

- Leaked the personal details of tens of thousands of FBI agents and US Department of Homeland Security (DHS) employees.
- Hacked into the AOL emails of CIA director John Brennan.
- Hacked into the personal email and phone accounts of the US spy chief James Clapper.
- Broke into the AOL emails of the FBI Deputy Director Mark Giuliano.

Federal officials haven’t yet released the identity of the arrested teenager, but the boy is suspected of being the lead hacker of Cracka With Attitude, who calls himself Cracka, the South East Regional Organised Crime Unit (SEROCU) told the Daily Dot.

According to the report, Cracka is the same teenage hacker who recently leaked the personal information of 31,000 government agents belonging to nearly 20,000 FBI agents, 9,000 Department of Homeland Security (DHS) officers and some number of DoJ staffers.

In a statement, the SEROCU confirmed that the unit had arrested a teenager on Tuesday in the East Midlands on suspicion of:

- Conspiracy to commit unauthorised access to computer material contrary to Section 1 Computer Misuse Act 1990.
- Conspiracy to commit unauthorised access with intent to commit further offences contrary to Section 2 Computer Misuse Act 1990.
- Conspiracy to commit unauthorised acts with intent to impair or with recklessness as to the impairing operation of a computer contrary to Section 3 Computer Misuse Act 1990.

The unit declined to provide any further information on the arrest, but while speaking to Motherboard, the arrested teenager denied being Cracka, saying "I am not who you think I am ;) ;) ;)"

"I am innocent until proven guilty so I have nothing to be

worried about," the teen said. "They are trying to ruin my life."

Neither the Department of Justice (DoJ) nor the FBI have yet responded to comment on it.

Google Wants To Save News Sites From Cyberattacks For Free

Mehdi Yahyanejad thought that after Iranians voted on June 12, 2009, he would finally get some rest. Yahyanejad, the editor-in-chief of the social news and citizen journalism site Balatarian.com, had been working around the clock to cover the election. So when hard-line President Mahmoud Ahmadinejad shocked the country by defeating reformer Mir Hussein Moussavi in a suspiciously large landslide, sending protestors flooding into the streets, the 33-year-old Iranian immigrant was on vacation in Big Sur, California. Instead of enjoying his summer holiday, Yahyanejad spent the next week locked in front of a computer, fighting to keep his site from getting crushed by a crippling cyberattack.

That digital bombardment, seemingly launched by the Iranian government to keep his site down during a critical political moment, was only the first of many. For years, every time there was new protest, the site got hit with a so-called distributed denial of service attack that flooded it with junk traffic to overwhelm its servers often preventing foreign media from accessing the photos and video of the unrest that Iranians posted on the site. Balatarin s staff blocked thousands of IP addresses a day and even brought in a Dutch cybersecurity consultant, to no avail. During an attack, any server we launched got shut down in a matter of minutes, Yahyanejad remembers. It was a pretty awful experience.

Then in May of 2013, one of Yahyanejad s contacts at Google suggested he sign up for a free trial of the company s Page Speed service, which caches websites on Google servers to give them faster loadtimes. He did, and the result was immediate. Suddenly, Balatarin was backed by Google s immense infrastructure. Its servers absorbed or filtered out the DDOS attacks, and Balatarin stayed online. It was a very sudden transformation, Yahyanejad says. We stopped worrying on those days of protest.

Google had quietly adopted Balatarin into an early pilot of a service called Project Shield. That service, designed to stop DDOS attacks from being used as a censorship tool, currently protects close to a hundred similar sites focused on human rights, election monitoring and independent political news. And now it s finally coming out of its invite-only beta phase to offer its free cyberattack protection to not just the most at-risk sites on the Internet, but to virtually any news site that requests it.

Today Google Ideas, recently renamed Jigsaw, is opening Project Shield to applications from any independent news site in other words, one that s not owned by a government or political party. Large corporate news sites are also eligible, but Project Shield team lead George Conard says the initiative s real target is small, under-resourced news sites that are vulnerable to the web s

growing epidemic of DDOS attacks. Just about anyone who s published anything interesting has come under an attack at some point, says Conard. The smaller and more independent voices often don t have the resources, whether technical or financial, to really put good protections in place That s where we come into the picture.

Any site that signs up for Project Shield can make a change to their domain name configuration that redirects visitors to a Google server. That server acts as a so-called reverse proxy an intermediate server owned by Google designed to filter out malicious traffic and cache some elements of the site to lighten the load on the website s own computers. (Conard was hesitant to describe any details of the service s filtering, to avoid giving tips to potential DDOS attackers.)

And what does Google, and its parent company Alphabet, get out of serving up its infrastructure resources for free to thousands of sites? Project Shield falls under Jigsaw s mission, as Alphabet executive director Eric Schmidt wrote last week, to use technology to tackle the toughest geopolitical challenges. Among Alphabet s collection of subsidiary organizations with a less-than-direct focus on profits, in other words, Jigsaw may be the least profit-focused of all.

 This isn t about revenue, says Jigsaw president Jared Cohen, a former staffer at the U.S. State Department who helped lead the agency s Internet freedom campaigns during the Arab Spring. He points to Google s larger mission statement, saying, When we talk about organizing the world s information and making it available and useful you have to make sure that once people have access to the information, it doesn t get DDOS attacked, it doesn t get compromised, it doesn t get censored in a politically motivated way.

Preventing DDOS attacks, Jigsaw engineers and execs argue, is good for the Internet. And what s good for the internet, they say, is good for Google. We just don t think that DDOS attacks should exist, Cohen says. We hope that Shield can do for DDOS attacks what Gmail did for spam.

Why News Sites Specifically?

For nearly a decade, DDOS attacks have been used as a form of just-in-time political censorship, as some Internet freedom analysts have called it. This is when, instead of blocking a site with a Chinese-style Great Firewall, governments or government-sponsored hackers will knock it offline at a crucial moment, like a protest or an election. And DDOS attacks have only become a more powerful and accessible method of censorship in recent years: DDOS-tracking firm Arbor Networks has found that attacks now routinely top 100 gigabits a second, compared with peak attacks of 50 gigabits a second in 2009.

That growing threat to the web led Google to launch Project Shield in 2013, and now to expand it to encompass any willing news site. Google chose to offer Project Shield specifically to news organizations because in many cases those groups depend entirely on their web presence to get information to the public, says early Project Shield product manager C.J. Adams. Project Shield is also open to human rights and election monitoring sites by invitation,

but Adams differentiates those categories of Shield users from news sites in that they re able continue their work even if their sites go offline.

News is also a broader and more easily defined category of sites than those others, Adams explains; Jigsaw will open Project Shield to news sites defined as those that would appear in Google News in other words, those with journalistic standards and attribution of reported facts. Individual bloggers and citizen journalism sites are welcome to apply, Jigsaw staffers say, but will be considered on a case-by-case basis.

They re careful to note, however, that the political slant or opinions of the site won t be used to discriminate who receives Shield s help. We ll protect people on all sides of a political dialogue, says Conard. One of the important things about keeping these voices alive is that you shouldn t be able to silence one point of view just by launching an attack.

Even this seemingly benevolent move by Google is sure to raise the eyebrows of the company s privacy critics, since involvement in Project Shield requires giving Google access to data about who visits a news site. But Jigsaw promises that the raw logs it collects from its reverse proxy service will be kept for a maximum of two weeks and then stored only in aggregate form to learn more about DDOS attack patterns. And it commits not to use any data it collects from Project Shield for advertising purposes. This comes up: What s the catch? What s in this for Google? says Adams. We ve made it very explicit we don t have the rights to commercialize anything that comes through.

Instead, Jigsaw argues that keeping news sites safe from DDOS attacks fits into Google s central purpose: to not just lead searchers to information, but to make sure it s online when they reach it. Is it worth it for us to spend the money and the bandwidth capacity to protect the world s news sites from getting DDOS attacked if that s something they want? Cohen asks. The answer for us is an obvious yes.

"Wow": Facebook Launches "Reactions" Worldwide

Facebook users around the globe can now do more than "like" a post. They can love it, laugh at it or feel angered by it.

The social network rolled out "Reactions" - an extension of the "Like" button - worldwide on Wednesday, to allow users to express sadness, wow, anger, love and laughter.

In a video accompanying a blog post, the five new buttons appear as animated emoticons that pop up when the "Like" button is held down on mobile devices. The buttons appear on desktops when users hover over the "Like" button.

Facebook launched a pilot of "Reactions" - which allowed users to select from seven emotions including "Angry", "Sad", "Wow" and "Like" - in Ireland and Spain in October.

The "Yay" emoticon, which was present in the pilot launch (http://on.fb.me/1LBnXIG), was not seen in Wednesday's video (http://bit.ly/24oZ6yi).

"People wanted to express empathy and make it comfortable to share a wider range of emotions," Zuckerberg wrote on his Facebook page.

Facebook Chief Executive Mark Zuckerberg said in September the company was thinking of adding a "dislike" button, which spearheaded a debate over whether it would increase cyber bullying and negativity on the site. In October, the company said it would expand its signature "Like" button with various reactions.

The slow test and rollout of the expanded button - which Zuckerberg has said is the company's biggest design change to date - is a marked change from Zuckerberg's famous mantra, "move fast and break things."

The company said it will also use "Reactions" to track user behavior and for ad delivery.

"We will initially use any Reaction similar to a Like to infer that you want to see more of that type of content," Facebook said in a separate blog post.(http://bit.ly/1TFzfOC)

The feature received mixed reviews from users on social networking sites.

Many complained that they could not see the new emoticons, while some were unhappy that Facebook did not launch a "dislike" button.

Marina Cupo wrote on Facebook: "I would rather have had a DISLIKE button and then attach an emotion instead if I want!"

Users have often responded negatively to similar changes on other sites. Twitter, for example, replaced its star-shaped "favorite" icon with a heart-shaped icon called "like" in November. Users initially scorned the change, but Twitter later said it increased activity on the site.

Siri for Mac Reportedly Coming This Fall, at Long Last

Apple put Siri, its voice-activated personal assistant, in the iPhone, iPad, Apple Watch, and Apple TV, but not the Mac. I assumed the company realized that people talking to their computers would be rage-inducing to those around them, but OS X has had dictation features for a while, and Apple has actually been testing Siri on the Mac for the last four years.

The feature is almost ready to go, 9to5Mac reported on Wednesday, and will be announced at the annual Worldwide Developers Conference as part of OS X 10.12 in June. The next version of the Mac operating system is likely to get a public release this fall.

So how will Siri on the Mac work? Kind of like Spotlight search, in that a Siri icon will sit in your menu bar until you need to use it. Click it, and a transparent overlay will pop up in the top

right of your screen with the same colorful waves you see on your iPhone screen, which indicates that Siri can hear you speaking. If your Mac is plugged in, you ll be able to say Hey, Siri and get a response without clicking.

It s unclear exactly why Apple waited so long to bring Siri to OS X, but according to 9to5Mac, the company may not have had a good idea of what it would be useful for (I m still skeptical, to be honest), or what the interface should look like. Those problems have reportedly been resolved.

Why this matters: Some have been waiting for years since Mountain Lion for Apple to put Siri in OS X. I don t get the appeal, but I m open to the idea if Siri proves to be incredibly useful on the Mac.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.